

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS:

1. (Currently amended) A method of securing access to resources in a computing device, comprising the steps of:
generating a random number on-chip during production of the computing device, such that the value of the random number generated on-chip is not known to anyone;
storing said random number in permanent memory in the computing device;
using the random number to generate an encrypted access code;
storing ~~thea~~n encrypted access code in a memory location within the computing device;
receiving a password to access the resources;
encrypting the password to produce a encrypted password;
comparing the encrypted password to the encrypted access code;
allowing access to the resources if the encrypted access code matches the encrypted password.

2-3. (Canceled)

4. (Original) The method of claim 1 wherein the encrypted access code is stored in a memory that cannot be externally modified.

5-6. (Canceled)

7. (Currently amended) A computing device comprising:
a permanent memory for storing a random number generated on-chip during production of the computing device, such that the value of the random number is not known to anyone;
a processing system; circuitry coupled to the permanent memory;
a memory coupled to the processing system for storing an encrypted access code
generated using the random number;
input circuitry coupled to the processing system for receiving a password to access resources;
wherein the processing circuitry:
encrypts the password to produce a encrypted password;
compares the encrypted password to the encrypted access code;
allows access to the resources if the encrypted access code matches the encrypted password.

8-10. (Canceled)

11. (Original) The computing device of claim 7 wherein the processing system allows access to testing resources if the encrypted access code matches the encrypted password.

12-13. (Canceled)

14. (Previously presented) The method of claim 13, wherein the processing system is a baseband processing system.

15. (Canceled)

16. (Currently amended) The method of claim 15 wherein the permanent memory ~~subsystem~~ comprises a memory array in which after data is written to the array, further writing to the particular memory location is disabled, such that the data cannot be overwritten.

17. (Canceled)

18. (Previously presented) The method of claim 16 wherein some portions of the memory array are externally accessible but not modifiable.

19. (Previously presented) The method of claim 16 wherein some portions of the memory array are not externally accessible and are not modifiable.

20-24. (Canceled)

25. (Currently amended) The method of claim 214, further including a radio frequency (RF) system coupled to the processing system.

26. (Canceled)

27. (Currently amended) The method of claim 167 wherein the ~~read-only-memory (ROM)~~ further comprises at least one of the following: ~~a program for determining whether boot system firmware is available for uploading at power up; a program for checking authenticity and integrity of the system boot firmware;~~ a program for preventing alternation of specific data associated with the computing device; a program for preventing alteration or swapping of firmware; cryptographic software.

28. (Canceled)

29. (Previously presented) The method of claim 1 wherein the encrypted password is of a different length than the received password.

30. (Previously presented) The computing device of claim 7 wherein the memory is a memory subsystem within the computing device.

31. (Previously presented) The computing device of claim 30 wherein the processing system, the memory and the input/output comprise a baseband processing system.

32. (Canceled)

33. (Currently amended) The computing device of claim ~~7~~³² wherein the permanent memory ~~subsystem~~ comprises a memory array in which after data is written to the array, further writing to the particular memory location is disabled, such that the data cannot be overwritten.

34. (Canceled)

35. (Previously presented) The computing device of claim 33 wherein some portions of the memory array are externally accessible but not modifiable.

36. (Previously presented) The computing device of claim 33 wherein some portions of the memory array are not externally accessible and are not modifiable.

37-40. (Canceled)

41. (Previously presented) The computing device of claim 31, further including a non-volatile memory system coupled to the baseband processing system wherein the non-volatile memory system is external to the processing system but internal to the computing device.

42. (Previously presented) The computing device of claim 41, further including a radio frequency (RF) system coupled to the baseband processing system.

43. (Canceled)

44. (Currently amended) The computing device of claim 35 wherein the read-only memory (ROM) further comprises at least one of the following: ~~a program for determining whether boot system firmware is available for uploading at power up; a program for checking authenticity and integrity of the system boot firmware;~~ a program for preventing alteration of specific data associated with the computing device; a program for preventing alteration or swapping of firmware; cryptographic software.

45. (Canceled)

46. (Previously presented) The computing device of claim 7 wherein the encrypted password is of a different length than the received password.